UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X
UNITED STATES OF AMERICA,

MEMORANDUM AND ORDER

- against -

24-CR-521 (GRB)

JACOB ISRAEL WALDEN,

Defendant.
----------X

GARY R. BROWN, United States District Judge:

Presently before the Court is a motion by defendant Jacob Walden seeking suppression of (1) evidence obtained from the manual and forensic search of his cell phone incident to an outbound border search and (2) the oral provision of his passcode and the fruits thereof. Docket Entry ("DE") 58. An evidentiary hearing was held on August 25, 2025, followed by submission of post-hearing briefs. After review, the Court finds that (1) the manual search of the defendant's phone was, under the facts of this case, a non-routine, intrusive search; (2) reasonable suspicion justified the manual and forensic searches under binding appellate precedent; (3) the Government acted in good faith, further justifying the searches and (4) the provision of defendant's passcode was voluntary. Therefore, for the reasons stated herein, defendant's motion is DENIED.

FACTUAL BACKGROUND

In or around September 2023, agents assigned to Homeland Security Investigations ("HSI") identified defendant as a potential purchaser of Child Sexual

Abuse Material ("CSAM") while engaged in a broader investigation into a CSAM enterprise. Hearing Transcript dated August 25, 2025 ("Tr.") at 18-21. That investigation identified a ringleader named Ryan Hine, who was involved in enticing underage girls to engage in sexual activities and producing and distributing CSAM. Tr. 18-19. Hine then advertised to "buyers both domestically in the United States and abroad" who purchased CSAM that was electronically distributed. Tr. 19. HSI Special Agent Christopher Moriarty, the lead investigator, identified defendant as one of these buyers through records of "payments in Venmo and Cash App" linked to defendant's name, date of birth, address and phone number. Tr. at 22. Moriarty then created an HSI "subject record" for defendant – officially identifying him as the subject of an investigation – which is automatically published to computer systems maintained by Customs and Border Protection ("CBP"). Tr. at 23-24. As a result, Moriarty automatically received travel notifications and learned that defendant planned international travel on three occasions in December 2023, January 2024, and February 2024. Tr. at 24-27. Due to scheduling conflicts, Moriarty did not encounter defendant on any of those occasions. *Id.* Moriarty then received a fourth notification that defendant would be traveling from JFK Airport to Italy at approximately 12:30 A.M. on April 21, 2024. Tr. at 28-29. Moriarty planned to intercept defendant while he was boarding his outbound flight. Tr. at 29-30.[1]

[1] Defendant argues that *Riley v. California*, 573 U.S. 373 (2014) should be extended to this case because it involves outbound, rather than inbound, searches, and misstates Second Circuit caselaw in this regard. *See* DE 58 at 24, 11 n. 1 (suggesting that the Court of Appeals rejected the Supreme Court's guidance on this issue in *Californaia Bankers Ass'n*

Late on April 20, 2024, Moriarty and Special Agent Chris Gnall arrived at JFK Airport, and a CBP agent escorted them to the jetway. Tr. at 31-32. Defendant and his family scanned their boarding passes and entered the jetway in anticipation of boarding the flight to Italy, at which time they were confronted by Moriarty. Tr. at 31, 122-3. Moriarty introduced himself, examined defendant's passport to verify his identity and then explained that "[defendant] and all of his merchandise . . . were subject to search and inspection." Tr. at 37-39. Moriarty then asked defendant and his wife if they had any electronic devices. Tr. at 39. Defendant and his wife, Rachel Walden ("Rachel"), produced their cell phones to Moriarity and provided their passcodes upon his request. Tr. at 40. Moriarty first unlocked Rachel's phone and took a picture of the "settings" screen which identified her as the phone's owner. Tr. at 42.

After returning Rachel's phone, Moriarty began a manual review of defendant's phone. Tr. at 44. Scrolling through a few screens, Moriarty observed several items which were relevant to the investigative information he had previously gathered, including a Cash App display name "Jake W" and tag $jakewny, identifiers for an account used for the acquisition of CSAM. Tr. 45-46. Second, the agent observed that

---

v. Shultz, 416 U.S. 21 (1974) as *dictum*). However, the Second Circuit has expressly rejected any distinction between outbound and inbound border searches. *United States v. Ajlouny*, 629 F.2d 830, 834 (2d Cir. 1980) ("[T]his Circuit [has held] squarely that the border search exception applies to items leaving as well as entering the country"); *United States v. Turner*, 639 F. Supp. 982, 986 (E.D.N.Y. 1986) ("The Second Circuit has clearly held that departing passengers and outgoing goods may be searched without the need for probable cause, a warrant, or even reasonable suspicion").

the phone was equipped with the Dropbox and Telegram applications, which Moriarity testified had been used to distribute CSAM by the subjects of his investigation. Tr. 47. Third, the agent observed a "fake calculator app," an application which "to the naked eye [] just scrolling through [appears] to be a calculator," but in reality allows the user to "surreptitiously [ ] hide photos, media, data, conversation, [and] even complete apps." Tr. at 47-48. The agent's familiarity with the fake calculator app arose from his work in investigating CSAM distribution in the past. *Id.*

At the agent's request, defendant produced his wallet, and Moriarty inspected the credit and debit cards found inside. Tr. at 49. Moriarty recognized defendant's credit card as the payment source for defendant's Cash App account. Tr. at 51. At that point, defendant asked why he was stopped, to which Moriarty responded that defendant "had been identified in an ongoing criminal investigation involving child exploitation and the purchase of [CSAM]." Tr. at 52.

Moriarty then inquired into whether defendant knew "Rosie Snow" or "Lacey Love." Tr. at 52-53. Rather than individuals, the investigation revealed that these "monikers" represented CSAM purchasers who were organized into groups. *See, e.g.* Tr. 189 (testimony that defendant "was identified as a purchaser that had paid into the Rosie Snow account."). Defendant responded that he knew these names represented groups of people. Tr. at 53. Moreover, Walden explained that he had been to "rehab," seemingly related to child pornography, and Rachel told Moriarty that she was aware of defendant's "issues." Tr. at 53-54. Shortly thereafter, Walden's young child became violently ill, prompting Moriarty to cease the encounter. Tr. at 55. Moriarty seized

defendant's phone and transported it back to HSI's office in Newark. Tr. at 61-62.

The next day, April 22, 2024, Moriarty provided the phone to a computer analyst who began creating a forensic extraction of all data on defendant's phone. Tr. at 62-63. The extraction was complete by approximately May 1, 2024, just over a week later. Upon review, Moriarty quickly discovered between 40 and 50 still images and another 40 to 50 videos of "clearly identifiable CSAM," as well as conversations regarding the purchase of thousands of other images and videos. Tr. at 63-64. Following this review, Moriarty and HSI: (i) sent administrative preservation notices to Cash App, Snapchat, and Omegle; (ii) identified and forensically interviewed minor victims; and (iii) contacted the United States Attorney's Office for the Eastern District of New York to present the matter for prosecution. Tr. at 65.

The agent believed that he had authority to review the materials obtained in the forensic extraction under aegis of a border search. Tr. 58, 99. After the filing of several district court decisions, in July 2024, Moriarty discussed with the United States Attorney's Office the possibility of applying for a search warrant for defendant's phone "out of abundance of caution" due to "specific cases where border search [authority] was being challenged in the Eastern District of New York." Tr. at 166. Special Agent Jaclyn Duchene then applied for a search warrant in the District of New Jersey (where the phone was located) on August 7, 2024. In that application, Duchene disclosed to the magistrate judge that the forensic extraction had taken place, and review had commenced, but she did not rely on that evidence from the forensic review to establish the requisite probable cause in support of the warrant. Tr. at 68. On August 7, 2024, a

United States Magistrate Judge signed the search warrant, and HSI agents continued to examine the forensic image of defendant's phone. Tr. at 70-71.

Neither defendant nor his wife, who witnessed much of this incident, testified at the hearing. Yet Walden submitted a declaration as part of his motion. DE 58-1. The Court cannot fully evaluate the credibility of his statements, which were not subject to cross-examination, and thus these statements carry less weight than live testimony. *United States v. Sultanov*, 742 F. Supp. 3d 258, 303 (E.D.N.Y. 2024) ("the Court credits and gives greater weight to Pichardo's in-person testimony, which was subject to cross-examination, than Sultanov's affidavit."). Yet certain assertions in the declaration provide helpful background on several points. Concerning his interaction with the agents at the jetway, defendant avers, in part, as follows:

> [The Special Agent] did not advise us that we were subject to an inspection of our luggage, personal items and person, although we had already been the subject of such an inspection and were not subject to a second inspection.
>
> He asked me if I was traveling with my nanny, and I told him that I was. He then said he wanted to talk to me and my wife.
>
> Based on his questions, I believed that he wanted to question us about our nanny's visa which we had helped her obtain.
>
> The agent then told me to take out my phone and give him the passcode. He told me I was not under arrest, but he needed to search me and my property.
>
> I gave him the passcode, believing that he wanted to find out information about my nanny's visa, which we had helped her secure.

DE 58-1 ¶ 4-11. Defendant then adds, without further explanation, as to providing the cell phone passcode that "I believed I had no choice." *Id.* ¶ 11. He further declared "I

told the agent that I knew 'Rosie Snow' to be a Snapchat username, but it was just that - a username, shared by a group of women who seek potential buyers for their digital content; however, Rose Snow was not a real person nor did I know anyone by that name." *Id.* ¶ 15. As to Rachel's statements, defendant declared "[m]y wife told him that she was aware of my 'demons' and was proud of the work I had done in recovery and that she has already supported me through rehab for my addictions." *Id.* ¶ 20.

DISCUSSION

A. Searches of Defendant's Cell Phone

The searches of defendant's cell phone present three questions. First, was the manual search of defendant's cell phone a routine search incident to a border search, thus requiring no suspicion on the part of the agents? Second, if the search was "non-routine," did the agent's reasonable suspicion to believe defendant was involved in procuring CSAM justify the warrantless searches conducted in this case? Third, assuming the searches improper, did the agent exercise the searches in good faith under *United States v. Leon*, 468 U.S. 897 (1984)?

According to the Second Circuit, "the Federal Government[] [has] broad plenary powers to conduct so-called 'routine' searches at the border even without 'reasonable suspicion that the prospective entrant has committed a crime.'" *United States v. Levy*, 803 F.3d 120, 122 (2d Cir. 2015) (quoting *Tabbaa v. Chertoff*, 509 F.3d 89, 97–98 (2d Cir. 2007), and citing *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) ("Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant...")). The Supreme

Court has "faithfully adhered" to the principle "that border searches were not subject to the warrant provisions of the Fourth Amendment and were 'reasonable' within the meaning of that Amendment." *United States v. Ramsey*, 431 U.S. 606, 617 (1977). Armed with reasonable suspicion, officers may conduct far more intrusive searches outside the purview of the Fourth Amendment. *United States v. Gavino*, No. 22-CR-136 (RPK), 2024 WL 85072, at *4 (E.D.N.Y. Jan. 7, 2024) ("[C]ustoms officers may conduct border searches that impinge significantly on privacy or dignitary interests when they have reasonable suspicion of criminal activity") (collecting cases).

1. The Nature of the Manual Search

Defendant, drawing on recent district court decisions, argues that "manual cell phone searches on the border are non-routine searches," thereby falling outside the ambit of routine searches that may be conducted without suspicion. DE 84 at 16-17 (citing *United States v. Sultanov*, 742 F. Supp. 3d 258, 290 (E.D.N.Y. 2024); *United States v. Fox*, 2024 U.S. Dist. LEXIS 130886, at *28-29 (E.D.N.Y. July 24, 2024);[2] and *United States v. Robinson*, 2025 U.S. Dist. LEXIS 89035, at *36-37 (E.D.N.Y. May 9, 2025)).

In response, the Government argues that a manual search of a cell phone categorically constitutes a "routine" border search requiring no individualized suspicion. DE 64 at 16-17 (citing, *inter alia*, *United States v. Mendez*, 103 F.4th 1303, 1307

[2] The determination in *Fox* is readily distinguishable as it turned, in large measure, on the fact that "the relevant officers were not searching for contraband or evidence of contraband." *United States v. Fox*, No. 23-CR-227 (NGG), 2024 WL 3520767, at *9 (E.D.N.Y. July 24, 2024), *appeal withdrawn sub nom. United States v. Cross-Mcknight*, No. 24-2262, 2024 WL 4925220 (2d Cir. Nov. 26, 2024). Here, the agent was searching for evidence and the existence of digital contraband on the subject device. Tr. 158.

(7th Cir. 2024) ("brief, manual searches of a traveler's electronic device are routine border searches requiring no individualized suspicion at all")); *cf.* Tr. at 208 (AUSA arguing that "there's no requirement for probable cause or reasonable suspicion to conduct a manual search. That's black-letter law."). The agent shared this view:

> Q. Based on your training and experience, do you have to have any level of suspicion to conduct a manual search of a device at the border?
>
> A. No. Per our agency policy and procedure, no.
>
> * * * * *
>
> Q. It's your understanding that you could stop anyone leaving the country or coming back in the country and search their electronic devices with or without probable cause, right, for any reason? To do a manual search.
>
> A. To do a manual, there's no suspicion [required].

Tr. 13-14, 147.

As the facts of this case demonstrate, both arguments are misplaced, glossing over important distinctions as to the extent of the manual search. The extent of a manual search can vary greatly, bearing on the appropriate analytical framework. The facts of this case provide excellent examples.

Consider the search of Rachel's phone. In this instance, as captured in both the testimony of the agent and an exhibit, it appears that he opened only the Apple ID (Account) Banner, which provides some identifying information about the owner, confirmed that the phone was hers, and returned the device. Ex. 102. As described in the testimony:

> Q. What did you do next?
>
> A. At that point, I started the initial inspection of Rachel Walden's phone. Then, I went in, I looked at -- just identified that it was, in fact, her phone that she was providing from her person. I took a photograph of the settings, showing that it was her phone. I then gave it back to her, thanked her.

Tr. 42. This effort seems consistent with a routine border search, as it appears minimally intrusive and furthered recognized governmental interests, *e.g*. ensuring that travelers are not transporting stolen property or items belonging to others. *See Ramsey*, 431 U.S. at 617(1977) (identifying "seizure of stolen goods" as one justification for border searches).

There is some caselaw support for the notion that such a limited manual search could qualify as a routine border search. In *Levy*, the Second Circuit considered:

> whether United States Customs officers at an international airport may lawfully and without a warrant examine and photocopy a document that belongs to a traveler entering the United States if the officers have reasonable suspicion on the basis of information supplied from another federal agency that the traveler is engaged in criminal activity unrelated to contraband, customs duties, immigration, or terrorism.

803 F.3d at 121. The document subject to search constituted a "spiral-bound notebook that contained eighteen pages of Levy's handwritten notes on various subjects, including travel information, business contacts, bank and trading account data, and limited details of Levy's personal affairs," which was reviewed and photocopied by customs agents during a border search, and formed part of the evidentiary basis of a securities fraud indictment of Levy which swiftly followed. *Id*. at 121-22.

In upholding the warrantless search in *Levy*, the panel noted that "[h]ad the CBP

officer merely skimmed the notebook and returned it to Levy without copying it, we have no doubt that the inspection would have been routine." *Id.* at 122. While *dicta*, this observation could provide support for the Government's contention that a limited manual search of a cell phone, under the right circumstances – like the search of Rachel's phone – might be deemed a routine search. *But see Gavino*, 2024 WL 85072, at *4 ("*Riley* thus establishes that even manual cell phone searches are intrusive.").

However, this authority – and the examination of Rachel's cell phone – stand in marked contrast to the manual search of the defendant's phone. Several exhibits – mostly screen shots taken from the defendant's phone that night, reflect some of the areas of the phone into which the manual search extended, including the Apple ID (Account) Banner and the Cash App account selection screen, accessed by scrolling through the Home Screens, identifying DropBox, Telegram and the fake calculator app, and opening the Cash App. Ex. 103, 104, 105. In his testimony, the agent testified that he intended to open the iPhone's Photos App to search for CSAM, but his manual search was interrupted when defendant's child became ill. Tr. 158.[3]

The agent's testimony failed to fully define the extent of the manual search, even though the Court raised this issue during the hearing. Tr. 209 ("how far does he get to go before it's something beyond [a] manual search that is superficial in nature?"). The following colloquy about the *faux* calculator app – a potentially significant piece of

[3] This testimony, which the Court credits, undermines defendant's arguments that the agent was not searching for digital contraband. DE 84 at 7 ("nor was there any search (physically, manually, or digitally) for contraband during this supposed 'border' action.").

evidence[4] - further demonstrates the absence of detail in the agent's testimony and the exhibits concerning the intrusiveness of the manual search:

> THE COURT: Is there something different about the icon that alerted you to that, or did you have to hit the icon to figure that out?
>
> THE WITNESS: It's -- I can't remember specifically.
>
> THE COURT: You don't have a picture of it here?
>
> THE WITNESS: I don't have a picture of it here.

Tr. at 48.

Yet, in this case, the evidence unquestionably shows that the manual search of defendant's phone was non-routine and hence intrusive. Thus, the analysis turns on the question of reasonable suspicion.

2. Reasonable Suspicion And the Searches of Defendant's Cell Phone

As the manual and forensic search of the defendant's phone were non-routine, warrantless border searches, the Court must determine whether the agent had

---

[4] The fake calculator app – a device designed specifically to conceal photos and other computer files – distinguishes this case from several others reviewed by courts. The presence of an application intended to secrete information on a phone could, like a suitcase with a false bottom or a vehicle with a secret compartment, bears upon the propriety of a more intrusive search. *See, e.g., United States v. Stephenson*, 452 F.3d 1173, 1176-77 (10th Cir. 2006) (noting that "an officer's observation of structural modifications to a vehicle can alone give rise to reasonable suspicion, and thus justify a stop, when the modifications are such that a well-trained officer may reasonably believe a crime is being committed" and "a hidden compartment . . . can contribute to probable cause); *United States v. Carrillo*, 269 F.3d 761, 767 (7th Cir. 2001) ("the existence of a trap coupled with other suspicious circumstances does create a level of suspicion sufficient to support a finding of probable cause.").

reasonable suspicion that defendant was engaged in CSAM activity sufficient to justify this intrusion.

Here, *Levy*'s holding appears dispositive. In denying a motion to suppress the photocopy of the notebook, the district court had held that the search "was a 'non-routine' border search because '[t]he close reading and photocopying of an entrant's documents goes beyond the general searching one expects at a point of entry' and may 'intrude greatly on a person's privacy.'" *Levy*, 803 F.3d at 122, (quoting *United States v. Levy*, No. 11–CR–62 (PAC), 2013 WL 664712, at *6, *12 (S.D.N.Y. Feb. 25, 2013)). Nevertheless, the Court of Appeals ultimately upheld the district court's denial of a suppression motion because "the inspection was justified by reasonable suspicion." *Levy* at 123.[5] The Circuit reiterated:

> The Supreme Court has instructed that "the level of suspicion the [reasonable suspicion] standard requires is considerably less than proof of wrongdoing by a preponderance of the evidence, and obviously less than is necessary for probable cause." *Navarette v. California*, ––– U.S. ––––, 134 S. Ct. 1683, 1687, 188 L.Ed.2d 680 (2014) (quotation marks omitted). Reasonable suspicion requires only "a particularized and objective basis for suspecting the particular person stopped of criminal activity." *Id.*

Id. The Circuit held that the customs agents had the right to rely on information

[5] The panel in *Levy* declined to reach the question of whether "searching *and copying* the notebook here constitutes a 'routine' border search that could be conducted without reasonable suspicion," a proposition it considered "somewhat more debatable." *Id.* at 123. Along with that observation, the panel cited, with approval, a Ninth Circuit case which upheld the search of a laptop without reasonable suspicion where "CBP officers simply had [the traveler] boot [the laptop] up, and looked at what [he] had inside." *Id.*, citing *United States v. Arnold*, 533 F.3d 1003, 1009 (9th Cir. 2008); *but see United States v. Cotterman*, 709 F.3d 952, 960 (9th Cir. 2013) (limiting *Arnold* decision, and finding reasonable suspicion does not support a warrantless forensic search of a computer).

developed in an ancillary criminal investigation conducted by agents from a different agency, finding that "interagency collaboration, even (and perhaps especially) at the border, is to be commended, not condemned" and that the validity of the search "does not depend on whether it is prompted by a criminal investigative motive." *Id.* (quoting *United States v. Irving*, 452 F.3d 110, 123 (2d Cir. 2006)). *Irving*, in turn, not only authorized the routine search of a traveler's belongings without any heightened suspicion but further sanctioned the non-routine search of computer discs and undeveloped film based upon reasonable suspicion of the defendant's involvement in child sexual abuse. *Id.*

Levy and *Irving* constitute binding appellate precedent applicable to the border searches in this case. Defendant would have this Court disregard such precedent based on his construction of the Supreme Court's decision in *Riley v. California,* 573 U.S. 373 (2014). DE 84 at 18 (describing *Riley* as a jurisprudential "sea change") and 16 (quoting amicus brief critical of *Levy*). Along those lines, the district court in *Smith* suggested that cell phone searches at the border cannot be justified by reasonable suspicion because "the magnitude of the privacy invasion caused by such searches dwarfs that historically posed by border searches." *Smith*, 2023 WL 3358357 at *7. And yet, "border detentions may involve the use of such highly intrusive investigative techniques as body-cavity searches, x-ray searches, and stomach-pumping." *United States v. Montoya de Hernandez*, 473 U.S. 531, 551 (1985). As my colleague Judge Kovner correctly observed:

Riley's analysis of the intrusiveness of cell phone searches does not justify

> requiring more than reasonable suspicion for a cell phone search conducted at the border, because, as noted above, "courts consistently have deemed reasonable suspicion sufficient to justify even the most intrusive of nonroutine border searches, including body cavity and alimentary canal searches," *United States v. Kolsuz*, 890 F.3d 133, 141 (4th Cir. 2018); *see Irving*, 452 F.3d at 123–24. *Riley* does not suggest that cell phone searches intrude more greatly on privacy or dignity than strip searches, alimentary canal searches, or the like. In fact, past decisions have suggested that searches of the body intrude more significantly than searches of property. *See Flores-Montano*, 541 U.S. at 152; *Aigbekaen*, 943 F.3d at 728 (Richardson, J., concurring); *United States v. Touset*, 890 F.3d 1227, 1233 (11th Cir. 2018). Moreover, a person headed abroad can leave behind a cell phone or curate its contents, even if doing so is inconvenient; a traveler seeking to avoid an intrusive body search has no comparable choice. *See Touset*, 890 F.3d at 1235. It is therefore unsurprising that no appellate court has required a greater quantum of suspicion for cell phone searches at the border than the reasonable suspicion that suffices for sensitive searches of travelers' bodies. *See United States v. Cano*, 934 F.3d 1002, 1015–16 (9th Cir. 2019) ("[P]ost-*Riley*, no court has required more than reasonable suspicion to justify even an intrusive border search.").

Gavino, 2024 WL 85072, at *5.

Defendant further adopts an argument articulated in *Smith* that the Government's interest in conducting border searches for digital contraband is undermined by the ability of individuals to transmit such material across the border electronically. DE 58 at 27 (citing *Smith* at 673 F. Supp at 394). However, the notion that the availability of alternate routes of transmission undermines the Government's border search authority has long been rejected by the Supreme Court:

> The border-search exception is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country. It is clear that there is nothing in the rationale behind the border-search exception which suggests that the mode of entry will be critical. It was conceded at oral argument that customs officials could search, without probable cause and without a warrant, envelopes carried by an entering traveler, whether in his luggage or on his person. Tr. of Oral Arg. 43-44. Surely no different

> constitutional standard should apply simply because the envelopes were mailed not carried. The critical fact is that the envelopes cross the border and enter this country, not that that are brought in by one mode of transportation rather than another. It is their entry into this country from without it that makes a resulting search "reasonable."

Ramsey, 431 U.S. at 620–22.

Another flaw in defendant's position is that – even assuming defendant's exegesis of the Supreme Court's determination in *Riley* held sway – this Court is not empowered to substitute its reading of the law for binding precedent of the Second Circuit.[6] As one district court observed:

> this Court cannot disregard Second Circuit precedent on estoppel unless or until the Second Circuit overrules such precedent. *See, e.g., Monsanto v. United States,* 348 F.3d 345, 351 (2d Cir. 2003) (District courts and even subsequent Second Circuit panels "are required to follow" Circuit precedent even if it is in "tension" with subsequent Supreme Court precedent unless and until that case is reconsidered by our court "[the Second Circuit] sitting in banc (or its equivalent) or is rejected by a later Supreme Court decision."); *see also In re Application of Hanwei Guo,* No. 18-MC-561 (JMF), 2019 WL 917076, at *3 (S.D.N.Y. Feb. 25, 2019) ("A district court, however, must follow Second Circuit precedent 'unless and until it is overruled in a precedential opinion by the Second Circuit itself or unless a subsequent decision of the Supreme Court so undermines it that it will almost inevitably be overruled by the Second Circuit.'"), *aff'd sub nom. In Re Guo*, 965 F.3d 96 (2d Cir. 2020) (citations omitted).

James v. Venture Home Solar, LLC, 715 F. Supp. 3d 203, 215 (D. Conn. 2024); *United States*

[6] One district court case relied upon by defendant contends that "neither the Supreme Court nor the Second Circuit has yet addressed "the level of suspicion required for [a non-routine] search [of a traveler's cell phone at the border] to be reasonable under the Fourth Amendment (i.e., whether it may be conducted at the point of entry by border officials based on a mere showing of reasonable suspicion or whether it requires a warrant and probable cause)." *United States v. Sultanov,* 742 F. Supp. at 281. This assertion seems inconsistent with *Levy* and *Irving*.

v. Dupree, No. 16-CR-84 (ARR), 2016 WL 10703796, at *4 (E.D.N.Y. Aug. 29, 2016), *aff'd,* 767 F. App'x 181 (2d Cir. 2019) (noting, in a Fourth Amendment decision that "[d]istrict courts in this circuit have held that they must follow binding circuit precedent unless a subsequent decision of the Supreme Court so undermines it that it will almost inevitably be overruled by the Second Circuit"). Earlier this year, another judge in this district observed:

> "[A] movant bears a substantial burden when urging the district court to depart from binding Second Circuit precedent on the basis of an asserted intervening change in controlling law. For a district court to ignore binding Second Circuit precedent, it is not enough for a Supreme Court decision to be in tension with that precedent." *King v. Habib Bank Ltd.,* No. 20-cv-4322, 2023 WL 8355359, at *1 (S.D.N.Y. Dec. 1, 2023), motion to certify appeal denied, 2024 WL 3761821 (S.D.N.Y. Jan. 2, 2024) (citations omitted). "[T]he district court must follow Second Circuit precedent 'unless and until it is overruled in a precedential opinion by the Second Circuit itself or unless a subsequent decision of the Supreme Court so undermines it that it will almost inevitably be overruled by the Second Circuit.'" *Id.* (quoting *United States v. Diaz*, 122 F. Supp. 3d 165, 179 (S.D.N.Y. 2015)) (citation omitted).

Est. of Henkin v. Kuveyt Turk Katilim Bankasi A.S., No. 19-CV-5394 (BMC), 2025 WL 622546, at *1 (E.D.N.Y. Feb. 26, 2025). Thus, neither this Court's view, nor that of respected fellow jurists, can countermand the Second Circuit's decisions in *Levy* and *Irving*, which govern the outcome.

It is beyond any question that, when approaching defendant at the jetway, Moriarity had reasonable suspicion that the defendant had engaged in child pornography offenses. Prior to their encounter, the agent had identified four accounts maintained by the defendant that were being used to procure CSAM. At the time of the border search, the agent had in his possession subpoenaed records from Cash App

documenting some of the suspect transactions. Tr. 34-36. Thus, "the inspection was justified by reasonable suspicion." *Levy* at 123.

And the level of suspicion continued to heighten during their encounter, all of which preceded the seizure and forensic review of the device. These factors include: (1) the presence of the following applications on the cell phone: Cash App (with the suspect account identifiers), Dropbox, Telegram and the fake calculator app; (2) the credit cards found in the defendants wallets that had been used to purchase CSAM materials; (3) oral admissions by the defendant and his wife that he had been to rehab for "issues," presumably with CSAM; and (4) defendant's statements regarding the account names used by the CSAM conspiracy, which demonstrated his familiarity with its workings. These factors further support the seizure and forensic review of the device which, under existing caselaw, required only reasonable suspicion, and was not subject to the warrant requirement.

3. The Good Faith Exception

The Court concludes, under all the relevant facts and circumstances, that the warrantless searches of the defendant's cell phone constituted valid border searches. However, even assuming, arguendo, that the searches were subject to exclusion, the Court finds that the searches fall squarely within the good faith exception contained in *United States v. Leon*, 468 U.S. 897, 922 (1984). As the Second Circuit has held, "when the Government 'act[s] with an objectively reasonable good-faith belief that their conduct is lawful,' the exclusionary rule does not apply." *United States v. Zodhiates*, 901 F.3d 137, 143 (2d Cir. 2018) (finding that warrantless cell phone tracking not subject to exclusion

based on existing precedent notwithstanding the interposition of *Riley*) (quoting *Davis v. United States*, 564 U.S. 229, 238(2011)).

Here, the decisions in *Levy* and *Irving*, as well as more than two centuries of jurisprudence establishing the extraordinary breadth of border search authority, provided a solid foundation for the Government's actions. Notably, two of the district court cases upon which defendant principally relies denied motions to suppress based upon the application of the good faith exception. One noted that "the breadth of the 'border search exception' was still largely in place at the time of the search," a conclusion "further reinforced by the Second Circuit's decision in *United States v. Levy*." *United States v. Smith*, 673 F. Supp. 3d 381, 401-02 (S.D.N.Y. 2023); *United States v. Sultanov,* 742 F. Supp. 3d 258, 299 (E.D.N.Y. 2024) (similarly applying good faith exception).

Further supporting this determination is the agent's efforts to secure a search warrant after the emergence of new case law. Following the April 2024 search of defendant's cell phone, on July 24, 2024, judges in this district issued the *Sultanov* and *Fox* opinions, which raised questions about border search authority in this context. On August 7, 2024 —fourteen days later—the Government sought and obtained a search warrant, disclosing all of the relevant facts to the magistrate judge. *See* DE 59-1. The magistrate judge issued the warrant. *Id.*

While the warrant does not provide authority for conducting the search, which had largely been completed, it certainly bears upon the good faith of the agents in handling this matter. As the *Smith* Court held:

> the Court separately concludes that the good faith exception precludes suppression of the fruits of that search because the Government ultimately obtained a search warrant. The core good faith exception to the exclusionary rule applies where the Government reasonably relies on a duly issued search warrant, even if that warrant should never have issued. United States v. Leon, 468 U.S. 897, 913-18, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984). Here, much (though not all) of the Government's actual search of the copy made of Smith's phone occurred after a search warrant was issued by Magistrate Judge Aaron. Clark Decl. ¶ 14; Gov't Opp. at 3-4. True, the Government obtained that warrant after the initial search occurred, and in order to establish probable cause, the Government relied in its warrant application on information already obtained (in this Court's view, unlawfully) from Smith's phone. Clark Decl. ¶¶ 14-15. But it disclosed the relevant circumstances of the search -- including that CBP agents seized, copied, and began searching Smith's phone without a warrant at the border in order to further non-border related investigations of other government agencies -- to Magistrate Judge Aaron.

Smith, 673 F. Supp. 3d at 402–03. Much of the same could be said of the instant case. Though not required by the advent of new district court authority, the Government nevertheless took the prudent step of seeking a search warrant from a judicial officer with reasonable dispatch and fully disclosing all the relevant facts and circumstances to the magistrate judge. DE 59-1. Thus, while the warrant did not immunize any improper conduct, it does, on balance, tend to buttress the Court's finding of good faith of the Government in this matter.

B. Motion to Suppress Defendant's Passcode

Defendant also seeks suppression of his oral provision of his passcode to the agent as an alternative means to suppress the fruits of the cell phone searches. In *Gavino,* Judge Kovner rejected a nearly identical claim:

> The defendant is also not entitled to suppression on the theory that the evidence seized from his cell phone was the fruit of an involuntary statement—namely, his statement providing Officer Sottile with his cell

> phone passcode. Even non-custodial statements to law enforcement officers violate the Fifth Amendment when they are not "voluntary, i.e., the product of an essentially free and unconstrained choice by [their] maker." *United States v. Haak,* 884 F.3d 400, 409 (2d Cir. 2018) (internal quotation marks and citation omitted). A statement is involuntary if, "considering the totality of the circumstances, the free will of the [person making the statement] was overborne." *United States v. Washington*, 431 U.S. 181, 188 (1977); *see United States v. Kourani*, 6 F.4th 345, 351 (2d Cir. 2021).
>
> In evaluating the totality of circumstances, courts consider "(1) the characteristics of the accused, (2) the conditions of the interrogation, and (3) the conduct of law enforcement officials." *Haak*, 884 F.3d at 409 (*quoting Green v. Scully*, 850 F.2d 894, 901–02 (2d Cir. 1988)). The relevant characteristics of the individual include his "experience and background, together with [his] youth and lack of education or intelligence." *Green*, 850 F.2d at 902 (citation omitted). "[T]he conditions under which a suspect is questioned" include "the place where an interrogation is held, [] the length of detention ... [and] [t]he presence or absence of counsel." Ibid. Factors bearing on law enforcement officials' conduct—the "most critical circumstance"—"include the repeated and prolonged nature of the questioning or the failure to inform the accused of his constitutional rights, whether there was physical mistreatment such as beatings, or long restraint in handcuffs, and whether other physical deprivations occurred such as depriving an accused of food, water or sleep, or even of clothing for a prolonged period." *Ibid*. In addition, courts consider whether law enforcement used "psychologically coercive techniques such as brainwashing or promises of leniency or other benefits." *Ibid.*

Gavino, 2024 WL 85072, at *8.

Here, no relevant factors point toward suppression. In the defendant's declaration, he acknowledges that the agent specifically "told me I was not under arrest," and that "the plane would not leave without our family." DE 58-1 ¶¶ 7, 10. Nothing about the physical or temporal circumstances of the encounter suggest any sort of detention. Nor is there evidence that the defendant's will was overborne when providing his passcode: by his own admission, the defendant believed the encounter

had to do with the provision of information about the immigration status of his nanny. *Id.* ¶¶ 6, 11. There are no claims of any physical or psychological abuse or manipulation. Thus, the Court finds the statement was voluntarily made and the motion to suppress it is without merit.

CONCLUSION

Based on the foregoing, the defendant's motion to suppress is DENIED.

SO ORDERED.

Dated: Central Islip, New York
November 12, 2025

/s/ Gary R. Brown
GARY R. BROWN
United States District Judge